QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Thao Thai (CA Bar No. 324672)
thaothai@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
sb@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

William A. Burck (admitted *pro hac vice*)
williamburck@quinnemanuel.com
Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN JOSE DIVISION

CHASOM BROWN, MARIA NGUYEN, and WILLIAM BYATT, individually and on behalf of all similarly situated,

Plaintiffs,

v.

GOOGLE LLC and ALPHABET INC.,

Defendants.

Case No. 5:20-cv-03664-LHK

DEFENDANT GOOGLE'S NOTICE OF MOTION AND MOTION TO DISMISS COMPLAINT

The Honorable Lucy H. Koh
Courtroom 8 – 4th Floor
Date: December 4, 2020
Time: 1:30 p.m.

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

Please take notice that, on December 4, 2020 at 1:30 p.m. the undersigned will appear before the Honorable Lucy H. Koh of the United States District Court for the Northern District of California at the San Jose Courthouse, Courtroom 8, 4th Floor, 280 South 1st Street, San Jose, CA 95113, and shall then and there present Defendant Google's Motion to Dismiss (the "Motion").

The Motion is based on this Notice of Motion and Motion, the attached Memorandum of Points and Authorities, the accompanying Request for Judicial Notice, the Declaration of Andrew H. Schapiro and exhibits attached thereto, the pleadings and other papers on file in this action, any oral argument, and any other evidence that the Court may consider in hearing this Motion.

ISSUE PRESENTED

Whether the Complaint, along with the documents referenced and incorporated therein and judicially noticeable documents, show that Plaintiffs fail to state a claim upon which relief can be granted, thus warranting dismissal of the Complaint under Rule 12(b)(6).

RELIEF REQUESTED

Google requests that the Court dismiss the Complaint with prejudice.

DATED: August 20, 2020

Respectfully submitted,

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By */s/ Andrew H. Schapiro*
Andrew H. Schapiro
Attorneys for Defendant Google

TABLE OF CONTENTS

Page

I. PRELIMINARY STATEMENT 1

II. BACKGROUND AND PLAINTIFFS' ALLEGATIONS 4

A. Plaintiffs Consented to Google's Privacy Policy 4

B. The Privacy Policy Disclosed that Google Receives the Data 5

C. Google's Disclosures Do Not Suggest that Private Browsing Prevents Google from Receiving the Data from Services like Analytics or Ad Manager 6

D. Websites Choose to Embed Google's Analytics and Ad Manager Code to Allow Google to Receive Information Used to Provide Its Services 9

III. ARGUMENT 10

A. All Claims Should Be Dismissed Because Plaintiffs and the Websites Consented to Google's Receipt of the Data 10

1. The Websites Consented to Google's Receipt of the Data 10

2. Plaintiffs Consented to Google's Receipt of the Data 12

B. Plaintiffs Fail to State Wiretapping Claims for Additional Reasons 12

1. Plaintiffs' Wiretap Act Claim Should Be Dismissed Because Google Received the Data in the Ordinary Course of Business 12

2. Plaintiffs' CIPA § 632 Claim Should Be Dismissed Because the Data Is Not a "Confidential Communication" 13

C. Plaintiffs Fail to State Constitutional and Common Law Privacy Claims 14

1. Plaintiffs Fail to Allege a Reasonable Expectation of Privacy in the Data 15

2. Plaintiffs Fail to Allege a Highly Offensive Invasion of Privacy That Constitutes an Egregious Breach of Social Norms 16

D. Plaintiffs' Claims Are Barred by the Statutes of Limitations 19

IV. CONCLUSION 21

TABLE OF AUTHORITIES

Page

CASES

Belluomini v. Citigroup, Inc.,
No. CV 13-01743-CRB, 2013 WL 3855589 (N.D. Cal. July 24, 2013) 17

Cada v. Baxter Healthcare Corp.,
920 F.2d 446 (7th Cir. 1990) 19

Campbell v. Facebook Inc.,
77 F. Supp. 3d 836 (N.D. Cal. 2014) 4, 14

Chance v. Ave. A, Inc.,
165 F. Supp. 2d 1153 (W.D. Wash. 2001) 11

Ellul v. Congregation of Christian Bros.,
774 F.3d 791 (2d Cir. 2014) 19

Flanagan v. Flanagan,
27 Cal. 4th 766 (2002) 14

Fogelstrom v. Lamps Plus, Inc.,
195 Cal. App. 4th 986 (2d Dist. 2011) 17, 18

Fox v. Ethicon Endo-Surgery, Inc.,
35 Cal. 4th 797 (2005) 20

Garcia v. Enterprise Holdings, Inc.,
78 F. Supp. 3d 1125 (N.D. Cal. 2015) 12, 19

Grisham v. Philip Morris U.S.A., Inc.,
40 Cal. 4th 623 (2007) 20

Guillen v. Bank of America Corp.,
2011 WL 4071996 (N.D. Cal. Aug. 31, 2011) 19

Hernandez v. Hillsides, Inc.,
47 Cal. 4th 272 (Cal. 2009) 14

Hill v. Nat'l Collegiate Athletic Ass'n,
7 Cal. 4th 1 (1994) 15

In re Doubleclick Inc. Privacy Litig.,
154 F. Supp. 2d 497 (S.D.N.Y. 2001) 11

In re Facebook, Inc. Internet Tracking Litig,
956 F.3d 589 (9th Cir. 2020) 2, 14

In re Facebook, Inc., Consumer Privacy User Profile Litig.,
402 F. Supp. 3d 767 (N.D. Cal. 2019) 15

In re Google Assistant Privacy Litig.,
2020 WL 2219022 (N.D. Cal. May 6, 2020) 17, 18

In re Google, Inc.,
2013 WL 5423918 (N.D. Cal. Sept. 26, 2013) 13, 14, 17

In re Nickelodeon Consumer Privacy Litig.,
2014 WL 3012873 (D. N.J. July 2, 2014) 10

In re Yahoo Mail Litig.,
7 F. Supp. 3d 1016 (N.D. Cal. 2014) 15

Jablon v. Dean Witter & Co.,
614 F.2d 677 (9th Cir. 1980) 19

Lauter v. Anoufrieva,
2011 WL 13175659 (C.D. Cal. Nov. 28, 2011) 19

Low v. LinkedIn Corp.,
900 F. Supp. 2d 1010 (N.D. Cal. 2012) 16, 17

Moreno v. San Francisco Bay Area Rapid Transit Dist.,
2017 WL 6387764 (N.D. Cal. Dec. 14, 2017) 17

People v. Nakai,
183 Cal. App. 4th 499 (2010) 14

Plumlee v. Pfizer, Inc.,
2014 WL 695024 (N.D. Cal. Feb. 21, 2014) 20

Revitch v. New Moosejaw, LLC,
2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) 14

Smith v. Facebook, Inc.,
262 F. Supp. 3d 943 (N.D. Cal. 2017), *aff'd* 745 F. App'x 8 (9th Cir. 2018) 10, 12, 15

Yunker v. Pandora Media, Inc.,
2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) 17

STATUTES

18 U.S.C. § 2510(5)(a) 12

18 U.S.C. § 2510(5)(a)(ii) 3, 13

18 U.S.C. § 2511 3

18 U.S.C. § 2511(1) 3, 12

18 U.S.C. § 2511(2)(d) 10

18 U.S.C. § 2520(e) 19

Cal. Civ. Code § 3515 ..... 10, 15
Cal. Penal Code § 630 3
Cal. Penal Code § 631(a) 10
Cal. Penal Code § 632(a) 10
Cal. Penal Code § 632(c) 14

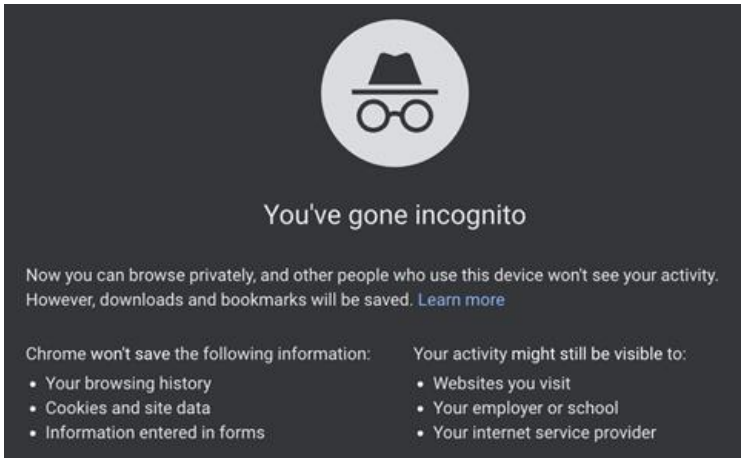
MEMORANDUM OF POINTS AND AUTHORITIES

I. PRELIMINARY STATEMENT

This case is predicated on a willful misreading of Google's disclosures. Plaintiffs quote snippets of Google's Privacy Policy and other disclosures out of context to argue that Google led them to believe that turning on their browsers' "private browsing" mode would prevent Google from receiving data generated by their internet browsing activity. But no plausible reading of Google's disclosures—including those quoted in the Complaint—supports Plaintiffs' purported belief.

Google Chrome is a web browser offering a "private browsing" mode known as "Incognito" that allows users to conceal their browsing activity from other people who may use their device. A user who plans to surprise her partner with a vacation to celebrate their wedding anniversary, for example, may use Incognito mode to ensure her partner does not discover that she was browsing the web for "Caribbean cruises." Incognito mode prevents previously-set cookies on the browser from being shared with the websites visited, in order to make the device appear as a new user. And the user's searches, browsing history, and cookies placed on the browser during the private browsing session that might be used to link the user's browsing activity to them or their device, are deleted when the Incognito session is closed. "Incognito" does not mean "invisible," however, and the fact that some unidentified user visited websites and reviewed certain pages is not hidden from the websites themselves, or from any third-party analytics or ads services they use.

This is all clearly disclosed in Google's Privacy Policy and other conspicuous disclosures regarding private browsing. Among them, *each time* a user enters Incognito mode, a *full-page* pop-up disclosure is displayed that describes private browsing and its practical effects in plain language:



Despite this clear disclosure, Plaintiffs argue that Google led them to believe private browsing would prevent Google from receiving the basic data Google needs to provide its Analytics and Ad Manager services to Websites, such as "IP address," URLs that identify "what [a] user is viewing," referral URLs that identify "what [a] user last viewed," and "search queries" (collectively, the "Data"). Comp. ¶¶ 3-5, 23, 27, 111. But Google's Privacy Policy—to which Plaintiffs consented when they signed up for their Google accounts—explains that Google receives *exactly* this Data:

> We collect information about the services that you use and how you use them, like when you … visit a website that uses our advertising services, or view or interact with our ads or content. This information includes: … details of how you used our service, such as search queries … internet protocol [IP] address… and referral URL.

Plaintiffs' contention that Google led them to believe that private browsing would *prevent* Google from receiving this Data is meritless. Consistent with the pop-up screen above, Google's other disclosures—quoted in the Complaint—explain that "although [p]rivate browsing works differently depending on which browser you use," it "usually means" that "[t]he searches you do or sites you visit won't be *saved to your device or browsing history*," and cookies placed on the browser during a private browsing session "are deleted *after* you close your private browsing window or tab." Compl. ¶ 33 (emphasis added). Plaintiffs' purported understanding that "Incognito" mode would render their browsing activity "invisible" is therefore contradicted by the very documents on which Plaintiffs rely.

Plaintiffs have transparently tried to conform their allegations to the Ninth Circuit's decision in *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020)—tracking parts of the decision verbatim, *see* Compl. ¶¶ 28 n.2, 39—but this case is nothing like *Facebook*. In *Facebook*, the Court held that the plaintiffs had stated wiretapping and invasion of privacy claims where Facebook allegedly (1) collected browsing history data from logged-out users notwithstanding its representation that, "[i]f you log out of Facebook, *we will not receive this information*," and then (2) "correlated users' browsing history *with users' personal Facebook profiles*—profiles that could include a user's employment history and political and religious affiliations[, giving] Facebook [] a cradle-to-grave profile without users' consent." *Id.* at 599, 602 (emphasis added). Here, in stark

contrast, Google did not represent that turning on private browsing would prevent Google from receiving the Data, and Plaintiffs do not allege that Google linked the Data *to them*. The fact that a webpage was visited or a search was made is not "private" information when that information is not linked to a particular user or account, and *Facebook* does not suggest otherwise.

The Complaint should be dismissed in its entirety with prejudice. *First*, Plaintiffs' wiretapping claims under the federal Wiretap Act, 18 U.S.C. §§ 2511, *et seq.* (Count I), and California's Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 630, *et seq.* (Count II), and their invasion of privacy claims under the California Constitution (Count III) and the common law doctrine of intrusion upon seclusion (Count IV), should *all* be dismissed because the parties to the "communications" that Google allegedly "intercepted"—*i.e.*, the Websites and Plaintiffs—consented to Google's receipt of the Data. The Websites clearly consented: Plaintiffs allege that the Websites "embedded" Google's Analytics and Ad Manager code for the *purpose* of allowing Google to receive the Data to provide website analytics and to serve ads. Compl. ¶¶ 22, 26. Because only one party's consent is necessary to defeat Plaintiffs' Wiretap Act claim, that claim should be dismissed based on the Websites' consent alone. Plaintiffs' remaining claims should be dismissed because they too consented to Google's receipt of the Data by consenting to Google's Privacy Policy, which disclosed that Google would receive the Data. There is no plausible argument that Google's private browsing disclosures negated that consent. To the contrary, Google's full-page pop-up window reminded users *every time they went Incognito* that private browsing meant simply that their activity would be concealed from other users of that device but would still be visible to a host of third parties.

Second, Plaintiffs' Wiretap Act claim should be dismissed because Google received the Data in the ordinary course of business. The Wiretap Act prohibits only the interception of electronic communications by a "device," 18 U.S.C. § 2511(1), and exempts from the definition of "device" one that is "being used by a provider of wire or electronic communication service in the ordinary course of its business," *id.* § 2510(5)(a)(ii). The "device" here is alleged to be the Analytics and Ad Manager "code" that, Plaintiffs allege, the Websites "embed[ed] … into their existing webpage code" in order to transmit the Data to Google so that the Websites could receive Google's Analytics

and Ad Manager services. Compl. ¶¶ 22, 26. Because Google's code was serving its intended business purpose, it does not constitute an intercepting "device."

Third, Plaintiffs' CIPA § 632 claim should be dismissed because, as courts in this district have held, "Internet-based communications are not 'confidential' within the meaning of section 632" given that they are typically recorded and "can easily be shared by … the recipient(s) of the communications." *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014).

Fourth, Plaintiffs' invasion of privacy claims under the California Constitution and the common law should be dismissed because Plaintiffs have alleged neither a reasonable expectation of privacy in the Data nor conduct by Google that even remotely amounts to an egregious breach of social norms, particularly given Plaintiffs' failure to allege that Google links the Data with them when they are in private browsing mode.

Fifth, all of Plaintiffs' claims should be dismissed because they are barred by the applicable one- or two-year statutes of limitations. Plaintiffs allege that they signed up for Google accounts more than four years ago and that Google has engaged in the alleged misconduct ever since. Compl. ¶ 8. Accordingly, their claims are time-barred unless an exception applies. But Plaintiffs' bare assertion that Google misled them and "[t]hey only learned of the truth in the weeks leading up to the filing of this Complaint" (*id.* ¶ 78), is insufficient to warrant application of the discovery rule, equitable tolling, or any similar doctrine. Plaintiffs could not possibly establish that such a doctrine applies given that (1) they consented to Google's receipt of the Data, and (2) they were shown a full-page pop-up screen that explained what private browsing means in Chrome *every time* they went Incognito. Accordingly, all of Plaintiffs' claims are time-barred and should be dismissed with prejudice.

II. BACKGROUND AND PLAINTIFFS' ALLEGATIONS

A. Plaintiffs Consented to Google's Privacy Policy

Plaintiffs "are Google subscribers whose internet use was tracked by Google between June 1, 2016 and the present." Compl. ¶ 8. By "tracked," Plaintiffs mean that Google "intercepted … communications made from the Plaintiffs to Websites other than Google in the form of detailed URL requests, webpage browsing histories, and search queries." *Id.* ¶ 111.

Although Plaintiffs allege that they have had active Google accounts and have been Gmail users for the proposed class period (beginning June 1, 2016), they conspicuously omit the dates they signed up for their accounts. *See id.* ¶¶ 79-91. The reasonable inference from the Complaint is that Plaintiffs signed up for their accounts at some point on or before June 1, 2016. *See id.* ¶ 8. During that time, Google required users to consent to its Terms of Services ("ToS") to create accounts.[1] Ex. 16 at 1.[2] The ToS, in turn, required Plaintiffs to consent to Google's Privacy Policy. *Id.* at 3. Google's ToS effective April 14, 2014 through October 25, 2017, for example, stated that "Google's privacy policies explain how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policies." *Id.* The words "privacy policies" are blue and hyperlinked so that the user can easily navigate to them. *Id.*

B. The Privacy Policy Disclosed that Google Receives the Data

Internet users provide a range of basic data to the sites they visit and receive content that is often paid for by advertising tailored to their online activity. Many Websites choose to use third-party services—such as Analytics and Ad Manager[3]—to analyze website utilization and serve ads. To do so, the Websites provide Google (or other third-party services) with information about activity on their sites. Often they do this by simply embedding code on the Website that directs visitors' browsers to send information directly to Google. Compl. ¶¶ 20-28.

This is not a case where Google received data surreptitiously, much less deceitfully. The Privacy Policy and other disclosures that Plaintiffs quote extensively (*id.* ¶¶ 29-32) disclosed that Google receives precisely this Data in the ordinary course. The Privacy Policy in effect at the

[1] The Court can take judicial notice of Google's ToS and Privacy Policies for the reasons explained in Defendants' concurrently filed Request for Judicial Notice. In addition, the Privacy Policies and other disclosures cited in the Complaint are incorporated by reference.

[2] All Exhibits cited herein are attached to the concurrently-filed Declaration of Andrew H. Schapiro.

[3] Plaintiffs allege that Google "accomplishes its surreptitious tracking" though "Google Analytics and Google Ad Manager." Compl. ¶ 4. Plaintiffs allege that Google also "tracks" users through "various other application and website plug-ins, such as … the 'Google Sign-In button' for websites." *Id.* ¶¶ 4, 42-49. The Complaint fails to explain, however, (1) how any purported "tracking" is achieved through these other means, or (2) whether Plaintiffs ever used any of these "other applications" or visited websites on which they were installed.

beginning of the class period (June 1, 2016), for example, stated: "We collect information about the services that you use and when you use them, like when you … visit a website that uses our advertising services, or view and interact with our ads and content." Ex. 3 at 2. The Privacy Policy specifically disclosed that Google receives each of the categories of Data at issue, including:

> device information … such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number….[;] Log information … [such as] details of how you used our service, such as your search queries … internet protocol [IP] address[;] device event information such as … the date and time of your request and referral URL[;] cookies that may uniquely identify your browser or your Google Account[;] Location information … [such as] IP address, GPS, and other sensors…[;] cookies and similar technologies to identify your browser or device.

Id. at 2-4. The Privacy Policy explained that Google receives the Data "when you interact with services we offer to our partners, such as advertising services or Google features that may appear on other sites," and "[o]ur Google Analytics product [that] helps businesses and site owners analyze the traffic to their websites and apps." *Id.* at 4.[4]

The Privacy Policy also explains an important distinction regarding when the Data is linked to a user's identity, and when it is not. The Data "may be associated with your Google account"—*i.e.*, the account of the individual user (which is linked to a person's name and other information at registration)—*if* you are browsing the web while "you are signed in to Google." *Id.* On the other hand, if the user is *not* signed in to a Google account—as Plaintiffs allege here, Compl. ¶ 95—Google still receives the Data from its services installed on third-party websites but uses "cookies or similar technologies to identify your browser or device." Ex. 3 at 4.

C. Google's Disclosures Do Not Suggest that Private Browsing Prevents Google from Receiving the Data from Services like Analytics or Ad Manager

Plaintiffs allege that Google led them to believe using a browser while in private browsing mode would prevent Google from receiving the Data. Compl. ¶ 57. Plaintiffs' "expectation" is

[4] Earlier and subsequent versions of Google's privacy policy contained identical or substantively identical disclosures. *See* Exs. 3-15. These Privacy Policies apply "to all of the services offered by Google Inc. and its affiliates, including YouTube, services Google provides on Android devices, and services offered on other sites (such as our advertising services)"—*e.g.* Google Analytics and Google Ad Manager. Exs. 3-7; *see also* Exs. 8-15 (containing substantially similar disclosures); *see also* Ex. 21 ("Safeguarding your data").

purportedly based on the Privacy Policy and other disclosures quoted in the Complaint, *id.* ¶¶ 29-36, but the documents on which Plaintiffs rely cannot be reconciled with any such expectation.

For example, Plaintiffs emphasize that Google's Privacy Policy linked to a page titled "Search & Browse Privately," which states generally that users are "in control of what information you share with Google when you search." Compl. ¶ 33. The next sentence lists several options: "[Y]ou can use private browsing, sign out of your account, change your custom settings, or delete past activity." *Id.* The page specifically explains "How private browsing works" generally, and states that, although "[p]rivate browsing works differently depending on which browser you use," it "usually means" that "[t]he searches you do or sites you visit won't be *saved to your device or browsing history*." *Id.* (emphasis added). The page further explains that "cookies" placed on the browser during a private browsing session—*e.g.*, by third-party websites, Google Analytics, or Google Ad Manager—"are deleted *after* you close your private browsing window or tab." *Id.* (emphasis added). Thus, although "you might see search results and suggestions based on … other searches you've done *during* your current [private] browsing session," the cookies linking those searches to the browser or device are "deleted after you close your private browsing window or tab." *Id.* (emphasis added). The page also makes clear that private browsing activity and searches are not associated with an individual user or account *unless* "you sign in to your Google Account" during the private browsing session, which Plaintiffs allege they did not do. *Id.* ¶ 33, 95.

Google has multiple other, clear disclosures explaining what private browsing means—and what it does not. The "Search & Browse Privately" page that Plaintiffs quote links to a page titled "How private browsing works in Chrome," which similarly explains: (1) "When you browse privately, *other people who use the device* won't see your history"; and (2) "Cookies and site data are *remembered while you're browsing*, but *deleted when you exit Incognito mode*." Ex. 19 (emphasis added). Users are informed that although "Incognito mode stops Chrome from saving your browsing activity *to your local history*[, y]our activity … might still be visible to: … websites you visit, *including the ads and resources used on those sites* [*e.g.*, Analytics and Ad Manager]";

"Websites you sign in to"; "Your internet service provider"; and "Search Engines."[5] *Id*. (emphasis added). And the page explains that, even in private browsing, "[a] web service, website, search engine, or provider may be able to see" "[y]our activity when you use a web service" and "[y]our IP address, which can be used to identify your general location." *Id*. Similarly, if a user clicks on the hyperlinked "Chrome" in the "Search & browse privately" page that Plaintiffs quote, the "Browse in private" page appears and describes "[w]hat happens when you browse privately," including that "Chrome won't save your browsing history, cookies and site data, or information entered in forms," and also makes clear that even when browsing privately, "[y]our activity isn't hidden from websites you visit, your employer or school, or your internet service provider." Ex. 20.

Google's Privacy Policies also provide a link to Google's Chrome Privacy Notice, which similarly explains how private browsing works in Incognito mode:

> You can limit the information Chrome stores *on your system* by using incognito mode or guest mode. In these modes, Chrome won't *store* certain information, such as: Basic browsing history information like URLs, cached page text, or IP addresses of pages liked from the websites you visit [and] Snapshots of pages that you visit.
>
> How Chrome handles your incognito or guest information[:]
>
> **Cookies.** Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new cookies on your system while you are in these modes, *but they'll only be stored and transmitted until you close the incognito or guest window*.

See, e.g., Ex. 17 at 7-8 (emphases added).

In addition, *each time* a Chrome user turns on Incognito, the full-page pop-up screen excerpted on page 1, *supra*, is displayed. Ex.1 (desktop view); Ex. 2 (mobile view).

In sum, Google's disclosures consistently stated that, in private browsing/Incognito mode: (1) "*other people who use this device* won't see your activity," (2) "*Chrome* won't *save*" the Data because, although "[c]ookies and site data are *remembered while you're browsing*, they are deleted

[5] The screenshot that Plaintiffs have pasted in paragraph 38 does not demonstrate any inconsistency between Google's disclosures and practices. Plaintiffs are correct that Google Analytics and Ad Manager may receive Data while the user is in private browsing, but, as the disclosures explain, the cookies to which that data is linked are deleted when the user closes out of their private browsing session. Plaintiffs do not allege that the data is associated with any particular device or user *after* they have closed the private browsing session.

when you exit Incognito mode," but (3) and "[y]our activity might still be visible to," among others, "[w]ebsites you visit."[6] Exs. 1-2; 19. Google disclosures do *not* state or even suggest that private browsing/Incognito mode prevents Google from receiving the Data through its services installed on third-party websites, such as Analytics or Ad Manager.

D. Websites Choose to Embed Google's Analytics and Ad Manager Code to Allow Google to Receive Information Used to Provide Its Services

The Complaint makes clear that Websites that want to make use of Google's services choose to embed Google's code for the purpose of transmitting the Data to Google so that Google can provide the desired services. Plaintiffs allege, for example, that the Websites choose to "embed Google's custom [Analytics] code into their existing webpage code" so that Google can receive "the user's IP address, URL address and particular page of the Website that is being visited"—*i.e.*, the Data—to provide the Websites "data analytics and attribution about the origins of a website's traffic, demographics, frequency, browsing habits on the Website, and other data about visitors." Compl. ¶¶ 20-23. Plaintiffs similarly allege that the Websites embed Google's Ad Manager code "into the Website's code" so that Google can receive the Data for the purpose of "tell[ing] the browser what Google advertisements to display [on the Website] along with the Website's actual content." *Id.* ¶¶ 26-27.

Plaintiffs allege that "Google does not require that Websites disclose upfront that Google is collecting the visitors' information." Compl. ¶ 23. Not so. Google's publicly available policies for Analytics and Ad Manager directly contradict that assertion: Google requires Websites to disclose all Google analytics and advertising services they have implemented, provide notice about what data will be collected, and whether this data can be connected to other data about the end user. *See* Ex. 22

[6] Plaintiff Nguyen alleges that Google also "intercepted" her browsing activity while she used private browsing mode in the Safari browser. Compl. ¶ 86. Google obviously cannot control, and is not responsible for, what Apple tells its users about what private browsing means. Nor is Google responsible for private browsing functionality in Safari. In any event, Google's Privacy Policy explains that "[p]rivate browsing works differently depending on which browser you use," but it "usually means" that "[t]he searches you do or sites you visit won't be *saved to your device or browsing history*." Plaintiffs do not allege that Apple made representations about private browsing in Safari that are inconsistent with Google's disclosures.

(Analytics Help Center) at 1; Ex. 23 (Analytics Protocol) at 1; Ex. 24 (Ad Manager Help Center) at 1; Ex. 25 (Platforms Program Policies).

III. ARGUMENT

A. All Claims Should Be Dismissed Because Plaintiffs and the Websites Consented to Google's Receipt of the Data

Plaintiffs allege that Google "intercepted" their "communications" with the Websites.[7] Compl. ¶ 111. But consent is a defense to each of their claims,[8] and here the parties consented to Google's receipt of the alleged "communications." Plaintiffs' Wiretap Act claim should be dismissed because only one party's consent is necessary to bar the claim and the Complaint makes clear that the Websites consented. Their remaining claims should be dismissed because Plaintiffs consented to Google's Privacy Policy, which disclosed that Google would receive the Data, and there is no plausible argument that the private browsing disclosures somehow negated that consent.

1. The Websites Consented to Google's Receipt of the Data

Because the Wiretap Act is a "one-party consent" statute, "it is not unlawful under the Act for a person to 'intercept … [an] electronic communication' … where one of the parties to the communication has given prior consent to such interception." *In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *13 (D. N.J. July 2, 2014) (quoting 18 U.S.C. §§ 2511(d)(2)). Because

[7] Elsewhere in their Complaint, Plaintiffs inconsistently allege that, as a technological matter, the "communications" were between their browser and Google directly, because: "[o]n websites with Google code such as Google Analytics and Ad Manager … Google's code directs the user's browser to copy the referer header from the GET Request and then send a separate but identical GET request and its associated referer header to Google's server." Compl. ¶ 28 & n.2. Even under that framing of the "communication," where Google is the intended recipient, all parties to the "communication" consented because Google disclosed that it would receive such information.

[8] *See* 18 U.S.C. § 2511(2)(d) (Wiretap Act) (it is not "unlawful … for a person … to intercept a[n] … electronic communication … where *one* of the parties to the communication has given prior consent to such interception") (emphasis added); Cal. Pen. Code §§ 631(a), 632(a) (CIPA) (prohibiting wiretapping and eavesdropping "without the consent of all parties to the communication"); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955-56 (N.D. Cal. 2017), *aff'd* 745 F. App'x 8 (9th Cir. 2018) ("Plaintiff's consent [] bars their common-law tort claims and their claim for invasion of privacy under the California Constitution.") (citing Cal. Civ. Code § 3515) ("He who consents to an act is not wronged by it.").

the communications at issue here were shared "with the express consent of websites" using Defendants' services, Plaintiffs' Wiretap Act claim fails. *See id.*

Plaintiffs' allegations establish that the Websites intentionally embedded Google's custom Analytics and Ad Manager code into each Website's code for the *purpose* of transmitting the Data to Google so that Google could provide its Analytics and Ad Manager services. Compl. ¶¶ 20-22 (Google Analytics); *Id.* ¶¶ 26-27 (Google Ad Manager).

Courts have long recognized that Websites that install Google's code to obtain services consent to Google's receipt of Data used to provide those services. In *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 503, 510 (S.D.N.Y. 2001), for example, the court held that Websites that used DoubleClick (which Plaintiffs allege is now known as Ad Manager, Compl. ¶ 25) to display ads had "consented" to DoubleClick's "interception" of Data generated by user interactions with those Websites—including "searches performed on the Internet [and] web pages or sites visited." In granting DoubleClick's Rule 12(b)(6) motion to dismiss, the court explained that it is "implausible to infer that the Web sites have not authorized DoubleClick's access" given that:

> Doubleclick-affiliated Web sites actively notify DoubleClick each time a plaintiff sends them an electronic communication (whether through a page request, search, or GIF tag). The data in these notifications (such as the name of the Web site requested) often play an important role in determining which advertisements are presented to users. Plaintiffs have offered no explanation as to how, in anything other than a purely theoretical sense, the DoubleClick-affiliated Web sites could have played such a central role in the information collection and not have authorized DoubleClick's access.

Id. at 510-11; *see also Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) ("It is implicit in the web pages' code instructing the user's computer to contact [defendant], either directly or via DoubleClick's server, that the web pages have consented to [defendant's] interception of the communication between them and the individual user.").

Because Plaintiffs allege that the Websites chose to embed Google's code for the purpose of transmitting the Data to Google, the Websites necessarily consented to Google's receipt of any Data. Plaintiffs' Wiretap Act claim should be dismissed on this basis alone.

2. Plaintiffs Consented to Google's Receipt of the Data

Plaintiffs, too, consented to Google's receipt of the Data. Plaintiffs allege that they have been Google account holders since June 1, 2016. Compl. ¶¶ 8-11. Therefore, they expressly consented to Google's Terms of Service and Privacy Policy. *See supra* at 4-5. The Privacy Policy specifically disclosed that Google would receive the Data, including through Analytics and Ad Manager. *See supra* at 6; *see also Smith v. Facebook, Inc.*, 745 F. App'x 8, 9 (9th Cir. 2018) (consent established for Wiretap Act and other claims given that "Terms and Policies contain numerous disclosures related to information collection on third-party websites"); *Garcia v. Enterprise Holdings, Inc.*, 78 F. Supp. 3d 1125, 1135-37 (N.D. Cal. 2015) (dismissing CIPA claim where app provider's terms and privacy policy provided consent for the alleged disclosures).

Plaintiffs' contention that, based on Google's private browsing disclosures, they understood they had *withdrawn* their consent by turning on private browsing, is meritless. As explained *supra* at 8, Google's disclosures—including the pop-up screen shown to Chrome users (like Plaintiffs) *each time* they turned on Incognito mode—made clear that private browsing means: (1) "*other people who use this device* won't see your activity," (2) "*Chrome* won't *save*" the Data because, although "[c]ookies and site data are *remembered while you're browsing*, they are deleted *when you exit Incognito mode*," but (3) "[y]our activity might still be visible to," *inter alia*, "Websites you visit." Exs. 1-2; 19. None of these representations suggests that private browsing would prevent Google from receiving the Data that the Privacy Policy disclosed Google ordinarily receives to perform its Analytics and Ad Manager services for Websites visited by Chrome users.

Because the parties to the alleged "communications" consented to Google's receipt of the Data, no additional analysis is required, and this Motion can be readily resolved: all of Plaintiffs' claims should be dismissed.

B. Plaintiffs Fail to State Wiretapping Claims for Additional Reasons

1. Plaintiffs' Wiretap Act Claim Should Be Dismissed Because Google Received the Data in the Ordinary Course of Business

The Wiretap Act prohibits the interception of electronic communications through an "electronic, mechanical, or other device." 18 U.S.C. § 2511(1). Section 2510(5)(a) exempts from

the definition of "device" any device that is "being used by a provider of wire or electronic communication service in the ordinary course of its business." *Id.* § 2510(5)(a)(ii). This Court has explained that this exception requires a "nexus between the need to engage in the alleged interception and … the ability to provide the underlying service or good." *In re Google, Inc.*, 2013 WL 5423918, at *11 (N.D. Cal. Sept. 26, 2013) (Koh, J.). That nexus is present here.

Plaintiffs allege that Google received the Data through Analytics and Ad Manager "code" that the Websites "embed … into their existing webpage code." Compl. ¶¶ 22, 26. Plaintiffs further allege that this "code" sends the Data "to Google and its servers." *Id.* ¶¶ 23, 27. Therefore, the "device" that allegedly transmits the Data to Google is the Analytics and Ad Manager "code" embedded in the Websites.

The "underlying service or good" (*see In re Google*, 2013 WL 5423918, at *11) in this case is analytics and ad services. Plaintiffs allege that Google's Ad Manager code "extracts" the Data in order "*[t]o display a webpage with an ad served by Ad Manager*." Compl. ¶ 27 (emphasis added). Plaintiffs similarly allege that Google's Analytics code is used to "provide[] data analytics and attribution about the origins of a Website's traffic, demographics, frequency, browsing habits on the Website, and other data about visitors." *Id.* ¶ 20. Plaintiffs do not (and could not) allege that Google could provide Analytics or Ad Manager services *without* receiving the Data.[9]

Accordingly, because Google's alleged "interception" of the Data is essential to its "ability to provide the underlying service[s]," *In re Google*, 2013 WL 5423918, at *11, the ordinary course of business exception applies and Plaintiffs' Wiretap Act claim should be dismissed.

2. Plaintiffs' CIPA § 632 Claim Should Be Dismissed Because the Data Is Not a "Confidential Communication"

A separate requirement under CIPA § 632 is the existence of a "confidential communication." *Id.* at *22. A communication is "confidential" for purposes of § 632 only if a

[9] For this reason, Plaintiffs' allegations are materially distinguishable from those at issue in *In re Google Inc.*, where this Court held that the ordinary course of business exception did not apply to Google's alleged "reading of [Gmail] user's emails" for the purpose of "creat[ing] user profiles and to provide targeted advertising" because "Google's interceptions are for Google's own benefit in other Google services unrelated to the service of email or the particular user." 2013 WL 5423918, at *8.

party "has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002); Cal. Pen. Code § 632(c). Plaintiffs fail to allege such an objectively reasonable expectation here.

"California appeals courts have generally found that Internet-based communications are not 'confidential' within the meaning of section 632, because such communications can easily be shared by … the recipient(s) of the communications." *Campbell*, 77 F. Supp. 3d at 849 (dismissing § 632 claim because Facebook messenger messages are not "confidential communications); *People v. Nakai*, 183 Cal. App. 4th 499, 518 (2010) (criminal defendant's intent to keep his internet chats confidential did not satisfy 632(a) because it was reasonable to assume that the communications could be recorded or shared by the service provider); *In re Google Inc.*, 2013 WL 5423918, at *22 ("Some decisions from the California appellate courts ... suggest that internet-based communication cannot be confidential [because] individuals cannot have a reasonable expectation that their online communications will not be recorded.").

Because Plaintiffs' internet-based communications are not "confidential communications," their CIPA § 632 claim should be dismissed. *See Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (dismissing § 632 claim because "browsing activity and form field entries" are not "confidential communications"); *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051-52 (N.D. Cal. 2018) (dismissing § 632 claim because even "emails and other electronic messages … concern[ing] private medical and financial information" are not "considered 'confidential' under CIPA") (quotation marks omitted).

C. Plaintiffs Fail to State Constitutional and Common Law Privacy Claims

"To state a claim for intrusion upon seclusion under California common law, a plaintiff must plead that (1) a defendant 'intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy,' and (2) the intrusion occurred in a manner high offensive to a reasonable person.'" *Facebook*, 956 F.3d at 601 (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (Cal. 2009)). "A claim for invasion of privacy under the California Constitution involves similar elements. Plaintiffs must show that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so

serious … as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *Id.* "Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Id.* Plaintiffs fail to plausibly allege either of these elements.

1. Plaintiffs Fail to Allege a Reasonable Expectation of Privacy in the Data

Plaintiffs fail to allege a reasonable expectation of privacy in the Data for two reasons: (1) Plaintiffs consented to Google's receipt of the Data; and (2) Plaintiffs do not plausibly allege that Google linked the Data *to them*.

First, Plaintiffs' constitutional and common law privacy claims fail at the outset because they consented to Google's receipt of the Data, as explained above. *See* II.A-C and III.A.2, *supra*. *See Smith*, 262 F. Supp. 3d at 955-56; *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1037-38 (N.D. Cal. 2014) (Koh, J.) (holding that a plaintiff asserting a privacy claim under the California Constitution "must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant") (quoting *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 26 (1994)); *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 792 (N.D. Cal. 2019) (dismissing sub-set of intrusion upon seclusion claims when disclosures could not "be interpreted as misleading users into believing that they merely needed to adjust their privacy settings to 'friends only' to protect their sensitive information from being disseminated"); Cal. Civ. Code § 3515 ("He who consents to an act is not wronged by it.").

Plaintiffs have tailored their claims to track the Ninth Circuit's decision in *Facebook*, where the Court held that users adequately alleged a reasonable expectation of privacy in their browsing history vis-à-vis Facebook while they were logged out of Facebook. 956 F.3d at 603-04. But the claims here do not fit *Facebook's* mold. Facebook's disclosures clearly stated that "[i]f you log out of Facebook, *we will not receive this information [i.e., browsing history]*." *Id.* at 602 (emphasis added). Relying on "Facebook's affirmative statements that it *would not receive information* from third-party websites after users had logged out," the Ninth Circuit held that "Plaintiffs have plausibly alleged that Facebook set an expectation that logged-out user data would not be collected," creating

a reasonable expectation of privacy that Facebook violated when it "collected [the data] anyway." *Id.* Here, by contrast, Google did not tell users that it would not receive the Data while users are in private browsing mode, and accordingly, Google did not create a reasonable expectation of privacy in the Data vis-à-vis Google.

Second, Plaintiffs do not have a reasonable expectation of privacy in the Data because they do not allege that Google links the Data to them. As Google's disclosures make clear, in Incognito mode: (1) previously-set cookies on the user's browser are not shared with the websites visited (and thus the device appears to websites and third party services on those sites, such as Analytics or Ad Manager, as a new user/device); (2) new cookies placed on the browser during a private browsing session are deleted when the session is closed; and (3) Google therefore does not associate the searches/browsing history conducted in a given logged-out private browsing session with an individual user or their device after the private browsing session is closed. Ex. 3; Ex. 17. Plaintiffs do not allege that Google acts contrary to these representations.[10] Plaintiffs' failure to make such an allegation is fatal to their ability to establish a reasonable expectation of privacy. Simply put, web browsing data disassociated from any individual user cannot support a common claim privacy claim. *See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (Koh, J.) (allegation that "browsing history" shared with third parties could be "de-anonymize[d]" insufficient to state invasion of privacy claim where plaintiffs did not allege "that anyone has done so").

2. Plaintiffs Fail to Allege a Highly Offensive Invasion of Privacy That Constitutes an Egregious Breach of Social Norms

The "California Constitution and the common law set a high bar for an intrusion to be actionable." *In re Google Assistant Privacy Litig.*, 2020 WL 2219022, at *19 (N.D. Cal. May 6,

[10] The closest that Plaintiffs come to making such an allegation is to suggest that, in theory, Google *could* "correlate [browsing history] with user, device, and browser IDs." Compl. ¶ 66; *see also id.* at ¶¶ 48-49 (noting Google's purported "*ability* to associate a particular user's online activity with his identity") (emphasis added). Plaintiffs do not explain how Google would accomplish this when users are logged out and in private browsing mode, and they appropriately stop short of alleging that Google actually does this. Moreover, even taking Plaintiffs' speculation about Google's capabilities as true, capability is not grounds for liability.

2020) (citation and quotation marks omitted). "Many courts have found that the collection—and even disclosure to certain third parties—of personal information about the users of a technology may not constitute a sufficiently 'egregious breach of social norms' to make out a common law or constitutional privacy claim." *Id.* (collecting cases); *see also In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014) ("Courts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms."). Plaintiffs have failed to adequately allege any invasion of privacy, let alone one so "highly offensive" as to constitute an "egregious breach of social norms."

First, courts in this district have held that disclosure of browsing histories or other personal data not linked to specific individuals does not constitute "a serious invasion of a privacy interest." In *Low*, for example, this Court held that the fact that the defendant allegedly "disclosed to third parties [the plaintiff users'] LinkedIn ID and URL of the LinkedIn profile page that the user[s] viewed (which in the aggregate disclosed users' browsing history among LinkedIn profiles)" did not constitute a "serious invasion of privacy" because "[a]lthough [p]laintiffs postulated that these third parties could, through inferences, de-anonymize this data, it was not clear that anyone had actually done so." 900 F. Supp. 2d at 1025; *see also In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 ("disclos[ure] to third parties [of] … the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices" … does not constitute an egregious breach of social norms") (citing *Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2d Dist. 2011)); *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) ("In this age of mobile technology the Court cannot conclude that a reasonable user would consider it highly offensive or egregious that a voluntarily downloaded mobile application which utilizes the user's cell phone identifier and location data when the app is in use, also 'periodically' accesses that anonymous data while the application is not in use.").[11] Indeed, "courts

[11] *See also e.g., Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (allegation that "Pandora obtained [plaintiff's] PII and provided that information to [third parties] for marketing purposes" not egregious); *Gonzales*, 305 F. Supp. 3d at 1092-93 ("Plaintiff consented to the sharing of his geolocation data with perfect strangers (Lyft riders); thus, under the circumstances he did not have a reasonable expectation of privacy in such information."); *Belluomini v. Citigroup, Inc.*, 2013 WL 3855589, at *6-7 (N.D. Cal. July 24, 2013) (permitting third

have characterized the collection and disclosure of browsing data as 'routine commercial behavior.'" *In re Google Assistant Privacy Litig.*, 2020 WL 2219022, at *19 (distinguishing "allegations that Defendants recorded their private conversations without authorization" from "browsing history" for purposes of invasion of privacy claim).

Second, Google's receipt of the Data was routine and served a legitimate commercial purpose. Plaintiffs conclusorily allege that Google uses the Data it receives through its Analytics and Ad Manager services for "nefarious purposes." Compl. ¶ 15. But courts have long understood that such web services "can serve legitimate commercial purposes." *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 294 (3d Cir. 2016); *id.* at 294-95 ("Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss."); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001) ("DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites."). And while a routine data collection "may be highly offensive if a defendant disregards consumers' privacy choices while simultaneously 'h[olding] itself out as respecting' them," *In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (citation omitted), Plaintiffs have failed to plausibly allege such circumstances here.

Plaintiffs' attempt to rely on the Ninth Circuit's *Facebook* decision to satisfy this element is misplaced. In *Facebook*, the Court held that the plaintiffs had adequately alleged a serious invasion of privacy where they alleged that Facebook acted surreptitiously in *direct contravention* of its privacy disclosures by "correlat[ing] users' browsing history with users' *personal Facebook profiles*—profiles that could include a user's employment history and political and religious affiliations," giving Facebook a "cradle-to-grave profile without users' consent." 956 F.3d at 598-

---

parties to access plaintiff's bank account and divulging her contact information was not a serious invasion of a privacy interest); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2d Dist. 2011), *as modified* (June 7, 2011) ("obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons" was "not an egregious breach of social norms, but routine commercial behavior").

99 (emphasis added). Here, by contrast, Plaintiffs (1) consented to Google's receipt of the Data, and (2) do not allege that Data received by Google while they are logged out and in private browsing mode is linked to them.

Plaintiffs' invasion of privacy claims should therefore be dismissed.

D. Plaintiffs' Claims Are Barred by the Statutes of Limitations

The statutes of limitations for each of Plaintiffs' claims is either one or two years.[12] Where, as here, the running of the statute of limitations "is apparent on the face of the complaint," a claim may be dismissed pursuant to Rule 12(b)(6). *Hakimi v. Societe Air France, S.A.*, 2018 WL 4826487, at *3 (quoting *Jablon v. Dean Witter & Co.*, 614 F.2d 677, 682 (9th Cir. 1980)).

Plaintiffs allege that Google has been intercepting their communications with Websites since at least June 1, 2016, Compl. ¶¶ 8, 95. Yet, they did not file their claims until June 2, 2020—years beyond the applicable statutes of limitations. Cognizant of this defect, Plaintiffs insist that "[t]hey only learned the truth [about Google's alleged misconduct] in the weeks leading up to the filing of this Complaint," and ask the Court to "toll" the limitations periods on their claims in light of Google's alleged misrepresentations to users regarding private browsing mode.[13] *Id.* ¶¶ 76-78.

[12] *See* 18 U.S.C. § 2520(e) (statute of limitations on Wiretap Claim is "two years after the date upon which the claimant first has a reasonable opportunity to discovery the violation"); *Brodsky*, 2020 WL 1694363, at * 16 ("Under the CIPA, the applicable statute of limitations is one year."); *Lauter v. Anoufrieva*, 2011 WL 13175659, at *7 (C.D. Cal. Nov. 28, 2011), aff'd, 550 F. App'x 473 (9th Cir. 2013) ("A claim for invasion of the California constitutional right to privacy has a statute of limitations of one year."); *Guillen v. Bank of America Corp.*, 2011 WL 4071996, at *10 (N.D. Cal. Aug. 31, 2011) (limitations period for intrusion upon seclusion is "one year in California").

[13] Plaintiffs conflate the doctrine of equitable tolling with the discovery rule. *See* Compl. ¶¶ 76-78 (requesting "tolling of the statute of limitations" on the basis that Plaintiffs allegedly "could not have reasonably discovered the truth about Google's practices"). "Equitable tolling is frequently confused … with the discovery rule. It differs from the [discovery rule] in that the plaintiff is assumed to know that he has been injured, so that the statute of limitations has begun to run; but he cannot obtain information necessary to decide whether the injury is due to wrongdoing and, if so, wrongdoing by the defendant." *Garcia v. Brockway*, 503 F.3d 1092, 1100 (9th Cir. 2007) (quoting *Cada v. Baxter Healthcare Corp.*, 920 F.2d 446, 451 (7th Cir. 1990) (Posner, J.)). The discovery rule, by contrast, "*delays* the date of accrual where the plaintiff is blamelessly ignorant of the existence or cause of his injury." *Ellul v. Congregation of Christian Bros.*, 774 F.3d 791, 801 (2d Cir. 2014) (emphasis in original). Plaintiffs appear to be claiming that they were unaware that they allegedly were injured, and thus that the discovery rule (not equitable tolling) applies. In any event, neither doctrine applies for the reasons explained in this section.

It is true that a plaintiff's reasonable reliance on a defendant's fraud to conceal a cause of action may toll the applicable statute of limitations. *See Grisham v. Philip Morris U.S.A., Inc.*, 40 Cal. 4th 623, 637 (2007). Here, however, Plaintiffs do not plausibly allege any "fraud" or "misrepresentation" by Google warranting tolling. As demonstrated above, Google's Privacy Policy—of which Plaintiffs received notice and consented—disclosed that Google ordinarily receives the Data from Google account holders like Plaintiffs. *See supra* at 5. Plaintiffs' allegation that Google's disclosures led them to believe that turning on private browsing would *prevent* Google from receiving the Data is rebutted by the very disclosures on which Plaintiffs rely. Accordingly, there is no basis to apply equitable tolling.

Nor does the delayed-discovery rule apply. Plaintiffs fail to satisfy their burden to "plead specific facts to show (1) the time and manner of discovery and (2) the inability to have made earlier discovery despite reasonable diligence." *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797, 808 (2005) (emphasis in original) (citation and quotation marks omitted); *see also Plumlee v. Pfizer, Inc.*, 2014 WL 695024, at *8 (N.D. Cal. Feb. 21, 2014) (Koh, J.) ("The burden is on the plaintiff to show diligence [warranting application of the discovery rule], and conclusory allegations will not withstand a motion to dismiss.").

Plaintiffs fail to satisfy the first element because they only vaguely allege that they "discovered the truth *in the weeks leading up to the lawsuit*," Compl. ¶ 78 (emphasis added), and make no allegations at all regarding the "manner" of discovery. *See Plumlee*, 2014 WL 695024, at *9 ("Even if such a general reference to the *time* of [plaintiff's] discovery [*i.e.*, "early 2012"] was sufficient," plaintiff's failure to "explain *how* she made the discovery at that time—*i.e.*, the *manner* of her discovery" precludes application of the discovery rule) (emphases in original).

Plaintiffs also fail to satisfy the second element because they do not allege that they were unable to discover Google's alleged misconduct despite conducting reasonable diligence. Indeed, Plaintiffs do not allege that they took even the most basic step of taking Google up on its offer, in the Privacy Policy, to "contact us" "if you have any questions" about Google's practices. *See* Ex. 3. Plaintiffs' lack of diligence is striking given that their Complaint cites publicly-available articles from 2018—*i.e.*, outside the limitations periods—as "evidence" of Google's purported misconduct.

See Compl. ¶ 47 (citing Aug. 15, 2018 paper); ¶ 52 (citing Nov. 1, 2018 article); ¶ 54 (citing May 10, 2018 article). This Court has rejected application of the discovery rule where, as here, "the Complaint identifies and relies upon several published articles" regarding the allegedly concealed facts "that were published many years before Plaintiff filed suit," and the plaintiff failed to "explain why she was unaware of these publications before 'early 2012' when she allegedly discovered the misrepresentation for the first time, nor explain[] why these publications did not serve to put her on notice that Defendant may have made misrepresentations."[14] *Plumlee*, 2014 WL 695024, at *9.

The law is clear that where, as here, "Plaintiff does not allege that she took *any* steps towards discovery," the discovery rule does not apply. *Id.* (emphasis in original). Accordingly, Plaintiffs' claims are barred by the applicable statutes of limitations and neither tolling nor the discovery rule can save them.

IV. CONCLUSION

For the foregoing reasons, the Court should dismiss this action in its entirety with prejudice.

DATED: August 20, 2020

QUINN EMANUEL URQUHART & SULLIVAN, LLP

By */s/ Andrew H. Schapiro*

Andrew H. Schapiro (*pro hac vice* pending)
andrewschapiro@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

[14] Any attempt by Plaintiffs to invoke the continuous accrual doctrine would be misplaced because "California courts have largely confined the application of the continuing accrual theory to a limited category of cases, including installment contracts, leases with periodic rental payments, and other types of periodic contracts that involve no fixed or total payment amount." *Brodsky*, 2020 WL 1694363, at *17 (citation and quotation marks omitted). "This court has repeatedly noted that when an alleged duty 'bears little relation to the monthly payments or monthly bills that California courts have found to be periodic, recurring obligations,' applying the continuous accrual doctrine is unwarranted." *Id.* (citation omitted). Nor does the continuing violation doctrine apply "to rescue … time-barred claims": "[T]he continuing violation doctrine applies *only* where 'a wrongful course of conduct [becomes] apparent only through the accumulation of a series of harms,'" "but not when a plaintiff experiences 'a series of discrete, independently actionable alleged wrongs.'" *Id.* at *18 (quoting *Aryeh v. Canon Bus. Solutions, Inc.*, 55 Cal. 4th 1185, 1199 (Cal. 2013)) (emphasis added).

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Thao Thai (CA Bar No. 324672)
thaothai@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

William A. Burck (admitted *pro hac vice*)
williamburck@quinnemanuel.com
Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
1300 I. Street, N.W., Suite 900
Washington, D.C. 20005
Telephone: 202-538-8000
Facsimile: 202-538-8100

Jonathan Tse (CA Bar No. 305468)
jonathantse@quinnemanuel.com
50 California Street, 22nd Floor
San Francisco, CA 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Attorneys for Defendant Google LLC